OFFICE OF INSPECTOR GENERAL

OIG

U.S. DEPARTMENT OF COMMERCE

Top 10 Management Challenges

September 2006

Major Challenges for the Department

This section highlights OIG's Top 10 Management Challenges that faced the Department at the close of this semiannual period. Each challenge meets one or more of the following criteria: (1) it is important to the Department's mission or the nation's well-being, (2) it is complex, (3) it involves sizable resources or expenditures, or (4) it requires significant management improvements. Because of the diverse nature of Commerce activities, these criteria sometimes cut across bureau and program lines. Experience has shown that by aggressively addressing these challenges, the Department can enhance program efficiency and effectiveness; eliminate serious operational problems; decrease fraud, waste, and abuse; and achieve substantial savings.

Top 10 Management Challenges

1. Strengthen Department-wide information security.
2. Effectively manage departmental and bureau acquisition processes.
3. Strengthen internal controls over financial, programmatic, and business processes.
4. Ensure that USPTO uses its authorities and flexibilities as a performance-based organization to achieve better results.
5. Control the cost and improve the accuracy of the decennial census.
6. Effectively manage the development and acquisition of environmental satellites.
7. Promote fair competition in international trade.
8. Effectively manage NOAA's ocean and living marine resources stewardship.
9. Aggressively monitor emergency preparedness, safety, and security responsibilities.
10. Enhance export controls for dual-use commodities.

Challenge 1

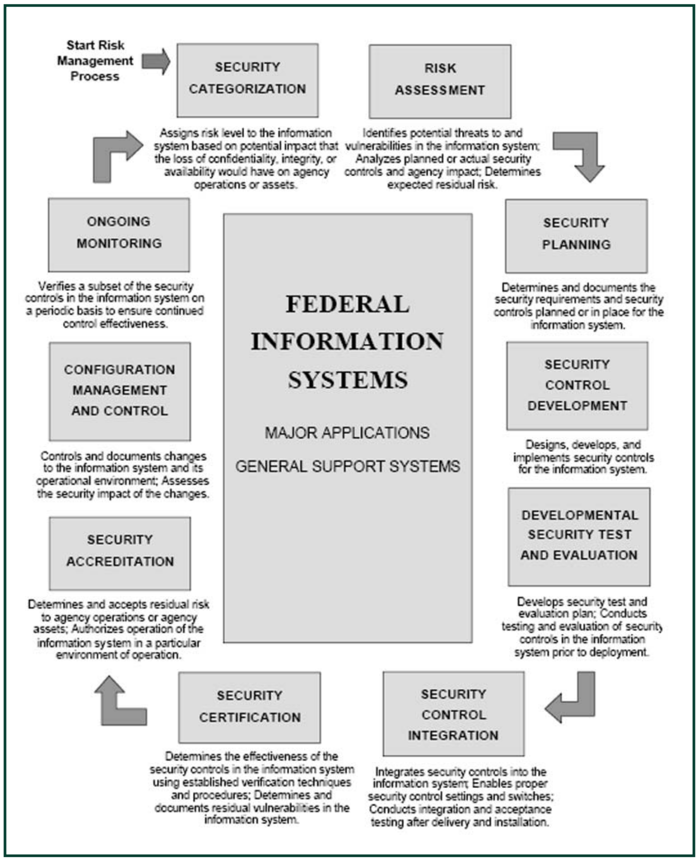
Strengthen Department-Wide Information Security

Since enactment of the Federal Information Security Management Act (FISMA), government agencies have devoted significant resources to improving the security of information stored on their computer systems. The problem is long standing: GAO has identified information security as a government-wide high-risk issue every year since 1997. At Commerce, it is the No. 1 challenge and has been a material weakness since 2001.

To eliminate the material weakness, Commerce has emphasized improving its certification and accreditation (C&A) process for IT systems. In February 2005, the chief information officer (CIO) issued a plan to produce acceptable quality C&A packages for all national-critical systems and some mission-critical systems by the end of FY 2005 and for all other systems by the end of FY 2006. In light of that plan, our approach to the C&A portion of our 2005 FISMA evaluation was to review all improved packages available by August 31, 2005. Only five were ready—three from NOAA and two from Census. Those packages showed some noteworthy improvements. However, with such a low number of packages available for review and considering the deficiencies we found, we concluded that the Department's C&A process had not improved to the point where authorizing officials had sufficient details about remaining system vulnerabilities to make fully informed accreditation decisions, and the IT security material weakness remained.

In early FY 2006, the acting CIO worked with the operating units to reassess the schedule and give units more latitude on time frames for completing improved C&A packages, which recognized that the amount of time necessary to complete the C&A process correctly had been continually underestimated. When revised schedules were finalized in June 2006, the Department's Office of the CIO (OCIO) expected a total of 28 C&A packages to be completed by the end of July, 27 of which were for high- or moderate- impact systems.[1] OCIO reviewed completed packages and worked with the bureaus to address concerns, as necessary. If OCIO determined a package was of sufficient quality, it was forwarded to OIG for FISMA review. As of August 24, 2006, our agreed-upon cutoff date, the CIO's office had received packages for 22 high- and moderate-impact systems, 12 of which were forwarded to us. We evaluated a total of 15 C&A packages for FY 2006 FISMA reporting. Eleven of these packages were Commerce-owned systems that had gone through the improvement process, and four

[1] Commerce systems were previously categorized as national critical, mission critical, or business essential. With the publication of NIST Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, agencies must now categorize information and information systems as low, moderate, or high impact, based on the potential consequences to organizations and individuals should there be a breach of security.



SECURITY CATEGORIZATION

Assigns risk level to the information system based on potential impact that the loss of confidentiality, integrity, or availability would have on agency operations or assets.

RISK ASSESSMENT

Identifies potential threats to and vulnerabilities in the information system; Analyzes planned or actual security controls and agency impact; Determines expected residual risk.

SECURITY PLANNING

Determines and documents the security requirements and security controls planned or in place for the information system.

SECURITY CONTROL DEVELOPMENT

Designs, develops, and implements security controls for the information system.

DEVELOPMENTAL SECURITY TEST AND EVALUATION

Develops security test and evaluation plan; Conducts testing and evaluation of security controls in the information system prior to deployment.

SECURITY CONTROL INTEGRATION

Integrates security controls into the information system; Enables proper security control settings and switches; Conducts integration and acceptance testing after delivery and installation.

SECURITY CERTIFICATION

Determines the effectiveness of the security controls in the information system using established verification techniques and procedures; Determines and documents residual vulnerabilities in the information system.

SECURITY ACCREDITATION

Determines and accepts residual risk to agency operations or agency assets; Authorizes operation of the information system in a particular environment of operation.

CONFIGURATION MANAGEMENT AND CONTROL

Controls and documents changes to the information system and its operational environment; Assesses the security impact of the changes.

ONGOING MONITORING

Verifies a subset of the security controls in the information system on a periodic basis to ensure continued control effectiveness.

Source: http://csrc.nist.gov/policies/WhatAgencycandonow-OMB-memo.pdf

were high- and moderate impact contractor systems that had not. (FISMA requires OIGs to review contractor systems.)

We found a larger percentage of C&A packages met the requirements of Commerce's IT security policy and applicable National Institute of Standards and Technology (NIST) standards and guidance (33 percent) as compared to last year (13 percent). But progress has been slow. Overall, we found that security plans and risk assessments have continued to improve. Security plans have shown particular improvement in the identification of network components. To be consistent with NIST standards and guidance and better support selection and tailoring of security controls, risk assessments now need to focus on specific threats and vulnerabilities for a given system instead of considering all possible risks.

We also found significant improvement in testing of the five systems we reported as certified and accredited, as well as in testing of a system granted interim authorization to operate. However, the remaining nine systems had serious deficiencies in the assessment of security controls, particularly in the testing of operational and technical controls needed to determine whether the security controls for network components are in place and operating as intended. That being the case, neither the certification agent nor the authorizing official had adequate information on the remaining vulnerabilities, and we again found this to be a material weakness within Commerce.

Our review included two draft C&A packages for USPTO contractor systems, which we found to be of poor quality. Therefore, we also recommended that USPTO, which submits its performance and accountability report separately, report IT security as a material weakness.

Protection of Sensitive Agency Information

After a recent series of incidents throughout the federal government involving the compromise or loss of sensitive personal information, the Office of Management and Budget (OMB) issued Memorandum M-06-16 on June 23, 2006. The memorandum emphasized the need to protect personally identifiable information that is remotely accessed or physically removed from an agency location, required agencies to ensure that appropriate safeguards were in place within 45 days, and asked inspectors general to conduct reviews.

OMB defines personally identifiable information as "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."[2]

OMB's memorandum included a checklist prepared by NIST for protection of remote information and recommended four additional actions: (1) encrypting all sensitive agency data on mobile computers/devices, (2) allowing remote access only with two-factor authentication,[3] (3) using a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity, and (4) logging all computer-readable data extracts from databases holding sensitive information and verifying such extracts have been erased within 90 days if no longer needed.

The President's Council on Integrity and Efficiency (PCIE) prepared a review guide for inspectors general and was to provide a government-wide report to OMB in October based on input from IG reviews of their agencies.[4] To evaluate Commerce, we selected a sample of 10 systems. This represents 16 percent of all systems identified by Commerce bureaus as storing or processing person-

[2] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 14, 2006.

[3] Two-factor authentication is achieved by authenticating two of the following three factors: 1) "something you know" (e.g. a password), 2) "something you have" (i.e. in your possession at the time of the authentication), or 3) "something you are" (e.g., a biometric such as your fingerprint)

[4] The PCIE was established by Executive Order 12805, May 11, 1992, to address integrity, economy, and effectiveness issues that transcend individual government agencies, and increase the professionalism and effectiveness of IG personnel throughout the government.

ally identifiable information and accessed remotely or physically removed from an agency location. We reviewed the current system security plan and all test results verifying that the applicable controls are in place for each of these systems.

Because of the short time available to perform our work (results were due to PCIE on September 22), our review was limited in scope, relying primarily on a comprehensive examination of security control test results provided by the operating units. Our FISMA work plan for FY 2007 includes actual testing of applicable security controls.

We found that in most cases bureaus could not demonstrate that the necessary steps have been taken to ensure that personally identifiable information is adequately safeguarded. None of the system documentation reviewed indicated that personally identifiable information was stored or processed, a step needed to determine the required safeguards. The Department's IT security policy does not explicitly address the protection needs associated with personally identifiable information that is accessed remotely or physically removed. The Department's OCIO has indicated that a revised policy addressing personally identifiable information requirements will be available during FY 2007. Most of the systems we reviewed showed no evidence that required protections for personally identifiable information transported and stored offsite, such as encryption, are implemented. There also was no evidence that protections are in place for remote access of personally identifiable information, such as virtual private networks or controls on downloading and storage of such data.

To address the loss of sensitive personal information from laptop computers and related equipment at the Census Bureau, the Secretary of Commerce asked OIG to determine the extent of problems in protecting sensitive personal information at Census, including whether property management policies and practices are adequate in light of the bureau's unique workforce and mission. We plan to report on the results of our evaluation in the next semiannual.

NOAA C&A

In this semiannual period, we reported on findings from our FY 2005 review of three NOAA C&A packages: the Search and Rescue Satellite-Aided Tracking system (SARSAT), the Polar Operational Environmental Satellite Ground System (POES), and the Office of Response and Restoration Seattle Local Area Network (Seattle LAN). Each of these systems was certified by NOAA personnel and accredited by a senior NOAA official as part of NOAA's C&A improvement effort.

Our report focused on two problem areas: incomplete system descriptions and inadequate security control assessments. Insufficiently complete system descriptions can yield inadequate identification and examination of system components in security control assessments. The security control assessments did not evaluate many of the system controls and were conducted without adequate test procedures. Consequently, NOAA's certification process did not provide sufficient information to authorizing officials on remaining system vulnerabilities.

In its response, NOAA stated that it had completed C&A activities for POES and SARSAT nearly 14 months ago, had made immediate changes to its C&A process after our December 2005 exit conference, and has implemented most of the changes recommended in our report. However, as we noted in our report, we prepared the report because some of the problems we identified in our FY 2005 and previous reviews were still evident in the additional five NOAA C&A packages we reviewed early in FY 2006. We hope that documenting our concerns in this report and making formal recommendations for improvement will facilitate complete correction of these issues, many of which have persisted for some time. (See page 33.)

NOAA E-Authentication

E-authentication is the process of electronically verifying the identities of users accessing government services over the Internet and is crucial to the Department's ability to properly authorize access to data and hold users accountable for their actions. We evaluated the quality of NOAA's e-authentication risk assessment and controls for SARSAT—the U.S. portion of an international program that uses satellites to coordinate search and rescue activities. These controls, implemented for two SARSAT web-based applications, provide a first line of defense for beacon registration data that is protected under the Privacy Act. According to NOAA's e-authentication risk assessment, one consequence of unauthorized use of the SARSAT beacon registration system is that search and rescue personnel could waste valuable time using incorrect or misleading data.

The objectives of our review were to determine if the risk assessment adequately identified the requirements for e-authentication controls and whether the controls had been implemented and properly certified prior to the system's accreditation. Our evaluation found that SARSAT's e-authentication controls do not provide adequate assurance of users' identities and recommended that NOAA redo the e-authentication risk assessment to better characterize and assess authentication risk, improve the system security plan to identify e-authentication requirements and appropriate controls, test controls, and take actions to correct deficiencies.

NOAA disagreed with our conclusion that SARSAT's e-authentication controls do not provide adequate assurance of users' identities, but agreed with all but one of our recommendations. After we clarified the meaning of that recommendation—to document any deficiencies identified as a result of performing e-authentication control testing—NOAA agreed with it as well. (See page 31.)

IT Security Clauses in Contracts

We conducted an evaluation to determine whether NOAA is incorporating the two information security clauses prescribed by the Department into contracts and to evaluate implementation of the clause requirements. Clause 73 requires contractors to comply with the Department's IT security policy and have their IT resources certified and accredited if they connect to a Commerce network or process or store government information. Clause 74 requires contractor personnel to undergo appropriate background screening and IT security awareness training.

We reviewed a judgmental sample of 16 NOAA service contracts and interviewed managers and staff from NOAA's Office of Acquisition and Grants, Office of the Chief Information Officer, and line offices. Because some problematic aspects of Clause 73 contributed to issues we identified at NOAA and in a previous review at USPTO, we also made recommendations to Departmental officials. Our report highlighted the need to clarify the requirement to include Clause 73 in all contracts in which contractor IT resources are either connected to a government trusted network or are allowed privileged access to government information. For the Department, the evaluation identified needed improvements to the IT security clause and the *Commerce Acquisition Manual* as well as the need for developing additional guidance to aid contracting officers and contracting officer representatives in their oversight of contractor information security. For NOAA we identified improvements needed for ensuring the certification and accreditation, as appropriate, of contractor IT resources.

Both the Department and NOAA agreed with our recommendations. On September 27, 2006, in response to our recommendations, the Department's director of acquisition management and procurement executive issued a procurement memorandum and *Commerce Acquisition Manual* notice with revisions to the clause and changes to the approach to determine the level of contract risk so that personnel receive background investigations commensurate with the risk level. (See page 35.)

Challenge 2

Effectively Manage Departmental and Bureau Acquisition Processes

Commerce spends nearly $2 billion annually on goods and services—roughly a third of its annual appropriation—and each year relies more on contractors to support its mission-critical work. Adequate oversight of acquisition planning and execution is essential to ensuring that taxpayers dollars are spent effectively and efficiently and procurement laws and regulations are followed.

For example, the Census Bureau's contracting for products and services to support 2010 decennial operations continues to bear watching. The bureau estimates that 17 percent ($1.9 billion) of its 2010 budget will be spent on contracts for information technology systems, advertising, and leases for local office space. One key IT program—Field Data Collection Automation (FDCA)—will develop the handheld mobile computers that field staff will use to collect 2010 decennial information. This is a critical piece of the bureau's reengineered strategy. Census originally planned to develop this equipment in-house but determined in early 2004 that it lacked the management and technical resources to do so, and on March 31, 2006, awarded a system development contract. However, the late decision to use a contractor and the initial slow pace in planning the acquisition shortened the amount of time available for awarding the contract and developing FDCA. This will delay address canvassing, the first major field operation of the dress rehearsal for the 2010 census.

Challenge 3

Strengthen Internal Controls Over Financial, Programmatic, and Business Processes

Internal controls are the steps agencies take to make sure their operations are effective, efficient, and in compliance with laws and regulations. Internal controls also ensure that financial reporting is reliable, and assets are safeguarded from waste, loss, or misappropriation, according to the Office of Management and Budget (OMB). Two documents, the Federal Managers' Financial Integrity Act (FMFIA) and the 2004 revision of OMB Circular A-123 (Management's Responsibility for Internal Control), set out internal control requirements for the federal government: Commerce and all federal agencies must define and document major financial internal control processes and test key financial controls to determine whether they are effective as of June 30, 2006.

Although we noted recent improvement in the Department's management and financial accountability as well as in program and operational effectiveness, our audits continually indicate more work is needed to strengthen internal controls over programs, operations, and administrative areas.

We expect the new federal emphasis on strong internal controls to create a number of new demands for OIG reviews in the coming years. For example, the Digital Television Transition and Public Safety Act of 2005 puts NTIA, one of the Department's smaller agencies, in a position of having to manage an enormous national project with an even larger budget than had been anticipated. Successfully implementing this act will constitute a significant management challenge for the Department. We will share lessons learned from our work in other areas to help the agency design strong, well-structured programs and minimize opportunities for fraud.

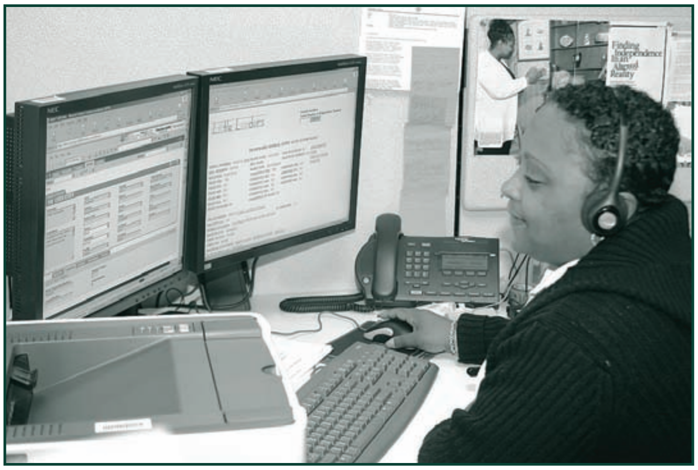
Challenge 4

Ensure that USPTO Uses Its Authorities and Flexibilities as a Performance-Based Organization to Achieve Better Results

Since March 2000 when the Patent and Trademark Office Efficiency Act transformed USPTO into a performance-based organization designed to operate more like a private corporation than a government agency, OIG has paid close attention to a number of aspects of the organization's internal management structures and practices.

USPTO faces numerous challenges, such as a continuing increase in applications, training about 1,000 newly hired examiners in Patents and Trademarks, and transitioning to an electronic processing environment. In addition, USPTO's expanded authority over personnel decisions and processes, procurement, and information technology operations needs to be effectively and efficiently utilized.

OIG has issued nearly a dozen reports examining problems at USPTO since 2001. The bureau has generally taken decisive action to address some problems we identified in the past, and we have been pleased that USPTO has been receptive to our recommendations. But ultimately, we believe that many of the problems USPTO suffers are serious and require the sustained commitment of senior managers to resolve. OIG will continue to monitor the bureau's progress.



A USPTO trademark information specialist assists customers.

Source: USPTO

Challenge 5

Control the Cost and Improve the Accuracy of the Decennial Census

Even after adjusting for inflation, the 2010 census will be the country's most expensive decennial ever—estimated to cost $11.3 billion. The Census Bureau's redesigned decennial plan, established after the 2000 Census, is heavily dependent on automating critical field operations to accurately count the nation's population within budget. The bureau has established a rigorous testing schedule to monitor development and implementation of the strategy, identify problems, and incorporate solutions in time for the decennial.

During the last 6 months, we built on the work we did in 2005 and early 2006, which reviewed the 2006 test's address canvassing operation. This semiannual report details our review of Census's test to enumerate the group quarters population (see page 19).

Although most U.S. residents live in residential housing units such as single-family houses, apartments, and mobile homes, more than 7 million people live in situations such as college dormitories, nursing homes, prisons, and group homes, collectively known as group quarters. We reviewed the group quarters testing operation at the Census Bureau's test site in Travis County, Texas. The area is ideal for testing the group quarters operation because it is home to four universities and colleges, a state prison, and numerous other group living facilities.

New Methods, New Challenges

Our review found that although the bureau is working on new methods to better enumerate the group quarters population, it continues to face a number of challenges. For example, nontraditional student housing, such as private dorms and student cooperative housing, did not easily fit into any of Census's group quarters definitions. Sometimes these units were defined as private residences and received housing unit questionnaires. In those cases, there was an increased likelihood that the unresponsive students had already moved out of their residence before the follow-up operation. When this occurred, enumerators relied on records kept in administrative offices, which often lacked Hispanic origin and race information. We also found that 42 percent of the validation workload was associated with large apartment complexes erroneously identified as potential group quarters during address canvassing. This caused problems in the group quarters validation and the nonresponse follow-up operations.

One of the objectives of our review was to independently assess the completeness of the group quarters listing prepared for the Census 2006 test. The bureau used four sources to develop a list of all potential group quarters for the 2006 test, which was then

Group Quarters Activities in the 2006 Census Test				
Operation	**Group Quarters List Development**	**Address Canvassing**	**Group Quarters Validation/Advance Visit**	**Group Quarters Enumeration**
Dates	June 2004—with updates throughout 2006 Census Test	July 2005—September 2005	December 2005—January 2006	April 2006—May 2006
Description	List created using • 2000 group quarters • Administrative records • Address canvassing (Other Living Quarters) • Other Census survey work	Identified potential "Other Living Quarters" (OLQs) Ensured addresses were correct and/or made changes to update the Master Address File	Listers visited 1,778 OLQs in Austin and 84 OLQs on the Cheyenne River Reservation to designate address status as a • GQ • Housing Unit • Nonresidential • Vacant • Transient • Duplicate • Other Group quarters administrators contacted regarding upcoming group quarters enumeration; privacy and confidentiality were discussed	Enumeration of all identified group quarters facilities

Source: U.S. Census Bureau, *2006 Census Test Project Management Plan,* 2010 Census Memoranda Series No. 8 (Reissue) December 2005

refined by the group quarters validation operation, resulting in a final list of group quarters to be enumerated. We found a number of group quarters that were not on the final enumeration list by conducting a limited Internet search and speaking with administrators. We also found duplicates—addresses that appeared on both the enumeration and housing unit lists or group quarters that appeared twice on the enumeration list. These errors can result in an inaccurate count of the population because individuals living in group quarters enumerated via the household questionnaire may be missed and duplicates on the list can result in people being counted twice.

We also found that Census should take additional steps to count the student population, such as working closely with fraternity and sorority campus oversight organizations and exploring the use of the Internet as a response option for this computer-oriented generation. Finally, we noted that some additional group quarters processes and procedures warrant management attention.

Looking Ahead

We continue to look at the update/enumerate operation at the Cheyenne River Reservation and Off-Reservation Trust Land in South Dakota. During this operation, which is used in communities where residents are less likely to return a completed questionnaire,

More than a dozen group quarters—and possibly many more—were not on the Census Bureau's enumeration list. This home is one of 15 missing from the list that we found by conducting a limited Internet search.

Source: OIG

enumerators update the address lists and maps and interview a resident to complete a questionnaire for each housing unit. We are assessing whether the update/enumerate operation obtained complete and accurate enumerations, especially with respect to large households, and if it resulted in improved address lists and maps. We are also assessing the bureau's method for designating which communities require this type of enumeration.

Challenge 6

Effectively Manage the Development and Acquisition of Environmental Satellites

Over the next 5 years, the Department, through NOAA, will spend several billion dollars in contracts for the purchase, construction, and modernization of environmental satellites.[5] These systems, operated by NOAA's National Environmental Satellite, Data and Information Service (NESDIS), collect data to provide short- and long-range weather forecasts and a variety of other critical environmental and climate information.

Complex, high-cost acquisitions such as these are extremely difficult to manage within cost and schedule goals, as was revealed in our audit during this reporting period of the National Polar-orbiting Operational Environmental Satellite System (NPOESS) (see page 29). This system—a joint project of NOAA, NASA, and Defense—is critical to the nation's ability to provide continuous weather and environmental data for civilian and military needs through the coming 2 decades. Initially projected to cost $6.5 billion, the program recently underwent a mandatory congressional review to see if it should be continued, given its troubling history of huge cost increases and schedule delays.

Congress Approves a Scaled-Back NPOESS Program

Last November, the Department of Defense reported that NPOESS costs had grown by 25 percent over original estimates—triggering the Nunn-McCurdy recertification provision of the FY 1982 National Defense Authorization Act. In addition to these staggering cost increases, the program was running 17 months behind schedule yet the contractor had received $123 million in incentive payments.

We sought to determine how cost and schedule overruns had grown so dramatically while the contractor had been so well rewarded. We identified serious shortcomings in the contract's incentive structure as well as in program oversight from NPOESS' executive committee, which consists of top leadership from NOAA, NASA, and Defense.

Source: http://goes.gsfc.nasa.gov/images/GOES-R_Color_Lg.jpg

Commerce IG Johnnie E. Frazier reported our findings to the House Science Committee in May (see page 50), as the recertification process was in progress. In June, the Committee accepted a triagency proposal to continue the program with the following changes:[6]

- Total acquisition costs were revised to $11.5 billion to support NPOESS satellite coverage through 2026.
- The number of satellites was reduced from six to four, with the U.S. relying on European satellites to fill in any gaps resulting from the reduction.
- The first satellite will launch in 2013 rather than 2010, as proposed in the original program.
- The number of sensors will drop from seven to five.
- Management reforms, including our recommendations for improving EXCOM oversight and revising the award fee contract, will be implemented.

This program will continue to bear close watching as it restructures and attempts to stay within its new cost and schedule goals, and we intend to follow its progress and keep Congress apprised of our findings.

GOES-R Costs, Schedule, and Capabilities Are Being Redefined

The GOES-R series is the next generation of geostationary satellites that will replace existing GOES satellites in the next decade. The new series will have enhanced sensing capabilities that are expected to offer an uninterrupted flow of high-quality data to support weather forecasting, severe storm detection, and climate research vital to public safety. GOES-R is a multicontract, mul-

[5] http://www.osec.doc.gov/bmi/Budget/05APPR/PAR05.pdf, page 210

[6] http://www.house.gov/science/hearings/full06/June%208/charter.pdf

tiyear program wholly funded by Commerce, though the new satellites will be developed and acquired with help from NASA. The Department's investment for GOES-R for fiscal years 2006 to 2010 is projected at about $2 billion.

Planning for the new series, which has been under way for the past 5 years, has given long and careful focus to the many risks inherent in developing satellite programs. Even so, the NPOESS experience has put new pressure on agency senior officials and program planners to have strong mechanisms in place for tracking every phase of the program and promptly mitigating problems that arise.

During this semiannual period, we initiated a joint review of the GOES-R program with NASA's Office of Inspector General. Our shared objective is to determine whether the Department and NASA have created a management structure to ensure effective oversight of the many risks associated with the GOES-R program. In preparing for the review, we learned that the Department, NOAA, and NASA are restructuring major aspects of the program as part of detailed risk reduction activities. GOES-R leadership is reassessing planned satellite capabilities and the timing of launches in response to input on costs and technological risks provided by an independent review team and contractors involved in defining the program's major aspects. In addition, program officials are considering changing approaches to managing the program and acquiring the satellites.

At Commerce, the oversight component of our work will look at the Department and NOAA's efforts to establish effective monitoring organizations, policies, and procedures and the mechanisms NOAA will use to leverage NASA's oversight expertise. We will also consider whether program staff report significant issues to senior Department and NOAA oversight officials in a timely fashion and whether those officials take appropriate action.

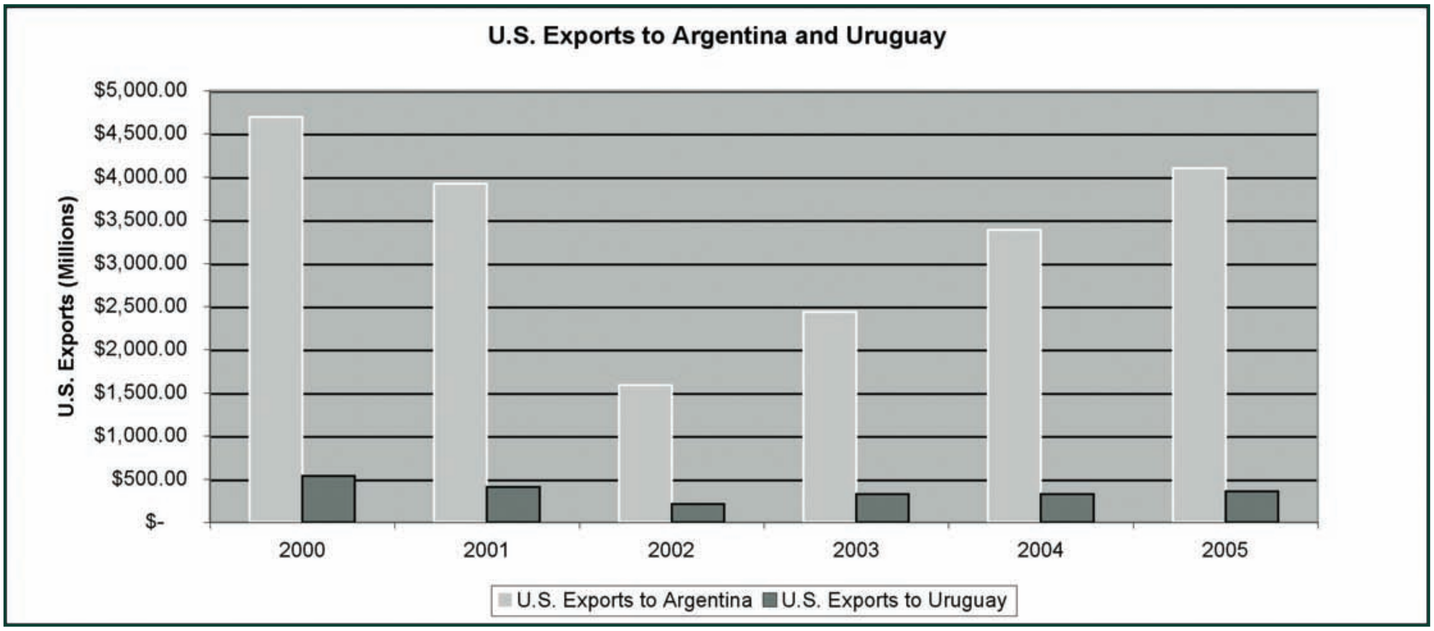
Our acquisition focus will be on the program office's overall approach to procuring key satellite instruments, identifying potential risks, and implementing associated mitigation strategies. We will also assess the acquisition contracts' award fee plans to determine whether they are structured to promote excellent performance.

NASA OIG plans to determine whether NASA program management councils effectively identify and review program issues and progress, and whether procedures and processes are in place to recognize, mitigate, and report technical risks in accordance with NASA policy.

Challenge 7

Promote Fair Competition in International Trade

The Department of Commerce accomplishes its goals of promoting trade, opening overseas markets to American firms, and protecting U.S. industry from unfair competition by imports primarily through the work of the International Trade Administration (ITA). ITA also works with USPTO and NIST to assist U.S. companies with intellectual property rights and standards. Over the past several years, OIG has focused a number of reviews on the Department's



Source: U.S. Census Bureau

efforts to increase U.S. market opportunities, provide assistance to U.S. exporters, and overcome trade barriers in difficult foreign markets.

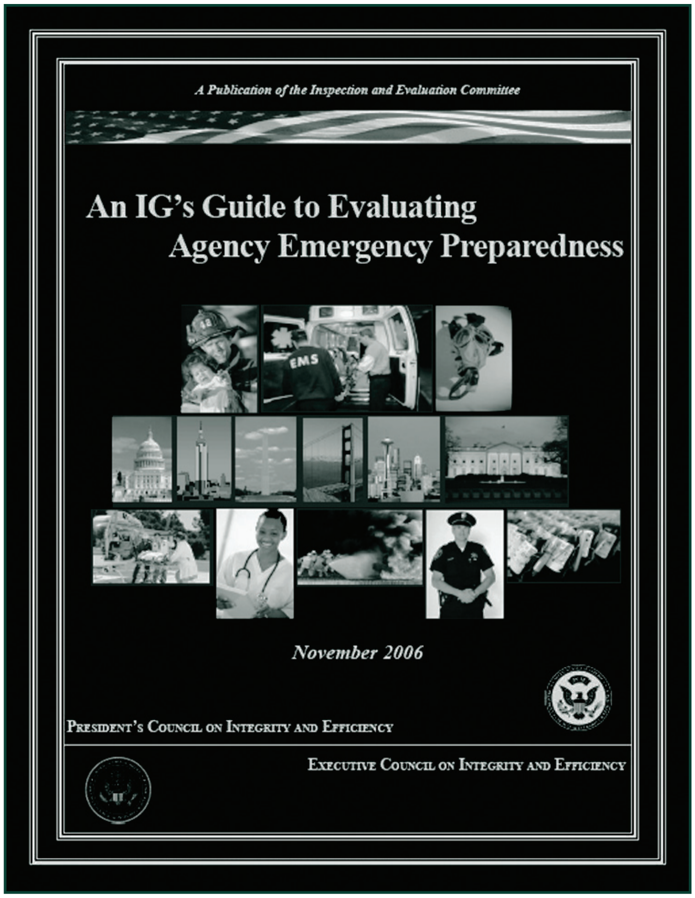
In September 2006, in response to OIG recommendations made to ITA in several recent reports, the bureau's Commercial Service (CS) announced extensive changes in its procedures for verifying export success claims, its primary performance measure. CS stated that the new procedures were necessary because, in a significant number of cases, OIG had found discrepancies in the reported export successes. These discrepancies raised doubts about the integrity of the data CS reports to Congress and the administration on its accomplishments. The new CS procedures require improved documentation, supervisory confirmation of a sample of export success reports, and verification that CS provided value-added assistance.

In response to a request from the House Small Business Committee, we are reviewing coordination and information sharing between Commerce and other U.S. government agencies with responsibility for trade promotion. The review, which we will discuss in our next semiannual report, will assess Commerce's efforts to match export opportunities with export-ready companies, with a focus on trade promotion agencies' use of the Internet to communicate leads and other relevant trade information.

U.S. Trade Promotion in South America

During this semiannual period, we conducted on-site inspections of CS posts in Brazil, Argentina, and Uruguay. Significant export opportunities are opening in these countries as Brazil's large economy continues its steady growth, Argentina recovers from its 2001-2002 economic crisis, and Uruguay pursues closer trade relations with the United States. Our inspections focused on the management, program operations, and financial and administrative practices of these three South American posts. We issued our report on CS' operations in Argentina and Uruguay in September with 20 recommendations, and we will publish our report on CS' larger post in Brazil before the end of the calendar year.

Our review of CS Argentina and CS Uruguay found that the posts are providing useful export assistance to U.S. companies and have established collaborative relationships with key U.S. government offices and nongovernmental organizations both in those countries and in the United States. Our review found effective administrative management practices at both posts, but we also identified some financial management and accounting concerns that warrant the attention of Commerce managers (see page 25).



A Publication of the Inspection and Evaluation Committee

An IG's Guide to Evaluating Agency Emergency Preparedness

November 2006

President's Council on Integrity and Efficiency

Executive Council on Integrity and Efficiency

Source: OIG

Challenge 8

Effectively Manage NOAA'S Stewardship of Ocean and Living Marine Resources

The National Oceanic and Atmospheric Administration is charged with monitoring the health of our nation's ocean, coastal, and Great Lakes resources; administering civilian ocean programs; and protecting and preserving the nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation.

During the past year, we followed up on our audit of the National Marine Fisheries Service's (NMFS') preparation of a biological opinion for California's Central Valley Project, one of the nation's major water conservation efforts. In response to our audit recommendations, NOAA received three reviews of the opinion. One review concluded that NMFS used the best scientific information for the biological opinion, but two reviews concluded that NMFS did not. In light of these findings, we asked NOAA officials to submit to us a plan that identifies actions they will take to address the deficiencies and implement the related recommendations made by the independent review organizations.

NOAA's future challenges include its efforts as a steward of marine resources, the agency's consultation process, and its management of fisheries and marine mammals.

Challenge 9

Aggressively Monitor Emergency Preparedness, Safety, and Security Responsibilities

The Department of Commerce has a dual responsibility in the area of emergency preparedness, safety, and security; not only must it be ready to protect 35,000+ employees and hundreds of facilities, but because several Commerce programs are critical to national preparedness and recovery efforts, it must support U.S. efforts to prepare for, respond to, and promote recovery from major disasters.

We continue to monitor Commerce's progress in resolving departmental emergency preparedness and security weaknesses we identified in assessments conducted in 2002 and 2005. Although Commerce has made significant improvement in emergency preparedness to address some of the vulnerabilities, we found, among other things, the need for better departmental guidance and oversight of emergency programs, risk assessments, occupant emergency plans, and security forces at its domestic operations, as well as better oversight of security upgrades and greater attention to security at its overseas offices.

More recently, in our review of the Commerce workers' compensation program, we recommended that the Department consolidate and analyze bureau safety data to help officials and managers identify and correct problems. We also recommended the Department use this data to find ways to help prevent workplace injuries and lower the number of employees who file claims for workers' compensation benefits.

Finally, we are working with other PCIE members to publish a guide for evaluating emergency preparedness programs. The guide should be a useful tool for conducting future OIG or management reviews of emergency preparedness in Commerce and other federal agencies.

These nuclear reactors are among 16 in operation throughout India, and the country has plans to build 6 more over the next 2 years. Under the terms of a July 2006 agreement, the United States will give India greater access to dual-use technology to expand its civilian nuclear program and meet its burgeoning energy needs.

Source: http://as.wn.com/i/d5/8c93997c11de00.jpg and http://www.icjt.org/npp/podrobnosti.php?drzava=11&lokacija=718

Challenge 10

Enhance Export Controls for Dual-Use Commodities

The Department's Bureau of Industry and Security (BIS) oversees the federal government's export licensing system for dual-use commodities and technology and is charged with advancing U.S. national economic security interests by administering and enforcing export controls. The primary goal of the licensing and enforcement system is to prevent hostile nations and terrorist groups from acquiring sensitive technologies and materials that have both civilian and military applications by controlling their export.

The National Defense Authorization Act (NDAA) for Fiscal Year 2000, as amended, directed the inspectors general of the departments of Commerce, Defense, Energy, and State, in consultation with the directors of Central Intelligence[7] and the FBI, to report to Congress by March 30, 2000, and annually until the year 2007, on the adequacy of export controls and counterintelligence measures to prevent the acquisition of sensitive U.S. technology and technical information by countries and entities of concern. (The Office of Inspector General at the Department of Homeland Security also has participated since its establishment in 2003.) In addition, the NDAA for FY 2001 requires

[7] The Intelligence Reform and Terror Prevention Act of 2004 [Public Law 108-458], dated December 17, 2004, established the Director of National Intelligence to serve as the head of the U.S. intelligence community.

the IGs to discuss in their annual interagency report the status or disposition of recommendations made in prior-year reports submitted under the act.

We have initiated our eighth and final NDAA required review, this time looking at the effectiveness of U.S. controls on dual-use exports to India. India presents unique challenges to U.S. commercial interests and export control policy. As one of the fastest growing economies in the world, India offers expanding trade opportunities for U.S. exporters but also increased competition for U.S. industry and labor.

We will detail the findings of our India evaluation in our March 2007 semiannual report. And though this will conclude our statutory reporting requirements under NDAA, we will continue to monitor BIS' efforts to implement and enforce dual-use export controls, given the importance of this mission to the nation's security. We will also follow up on our previous NDAA recommendations and report on BIS' progress in implementing them in our next semiannual report.

Some Export Control Topics Covered by Interagency OIG Reviews

Federal automated export licensing systems

Commerce Control List and U.S. Munitions List

Deemed exports

Export enforcement

Export licensing process for chemical and biological agents

U.S. dual-use export controls for China

U.S. dual-use export controls for India (Commerce only)